The Front Burner Cyber Security

The ACIO for Cyber Security

Issue No. 12

December 2009

Staying Safe While Shopping Online?

Tis the season of retail madness: *Black Friday*, *Cyber Monday*, and…*Hacker Tuesday*? Yes Virginia, it's true; Cyber criminals are celebrating this holiday season; only they won't be taking any time off to sample the eggnog. Like proverbial Scrooges, they will be online with the rest of us stalking the unsuspecting holiday shopper.

So what steps can you take to protect your identity and secure your online shopping experience this holiday season?

1 – Enable Security and Privacy Settings on Your Computer

One of the nice features of many computers we buy these days is that they come with some security built in to the operating system (e.g., Windows, Mac OS, Linux, and UNIX) and the Internet browser. You may also have additional security software that you purchased or that came with the computer. This software, as well as security and privacy settings in general, are not always turned on by default. Make sure you enable security and privacy features on your browser, operating system, and any program you may be using to protect your computer.

2 – Update Operating System and Security Software

Once you are sure your security/privacy software and settings are properly enabled, the next step is to update your operating system and security software (e.g., antivirus, firewall, etc.) with the latest software patches and updates. Unpatched computers are a hacker's favorite target and easiest way to gain access to your system. So before you go anywhere online, make sure your software is updated.

3 – Wired is Still Preferable to Wireless

Wireless computing can be secured; however, unless security is properly configured and you are connecting to the right network, there is a greater risk that you will be exposed through a wireless connection than with a wired connection. And recalling our tip from the last issue of the Front Burner, "turn off the wireless network card to avoid the possibility of inadvertently allowing access to your computer."

4 – Look for the Lock at the Bottom of Your Browser

When making payments online or entering in any personal information, including your username and password, a good rule of thumb is to make sure your browser displays a lock icon (typically at the bottom right-hand side) to indicate it is making a secure, encrypted connection. Another thing to look for is that the URL (website address) begins with "https://" rather than "http://". The "s" stands for "secure" and is critical for ensuring you have encrypted communication with the website from which you are making your purchase.

5 – Only Visit Sites You Know and Trust: Don't Leap At Every Bargain or Sale

In the end, it all comes down to trust, and some vendors on the Web are not legitimate. So no matter how good the bargain seems, stick with the vendors you know and trust. The best online vendors usually take extra care to protect your personal information. That extra touch may make the difference between a happy and a bah-humbug holiday.

DOE Headquarters Cyber Security Awareness Day is a HIT!

October was *National Cyber Security Awareness Month*. As part of an ongoing campaign to raise awareness of current threats and good computing practices within the DOE community, the DOE Office of the Chief Information Officer, Office of Cyber Security sponsored a Headquarters Cyber Security Awareness Day on October 22. The highlight of this event was the *Internet Survivor Challenge* where teams were tested on their ability to survive the Internet jungle.

Internet Survivor Challenge Winners!
Congratulations to the 2009 winners of the inaugural Cyber Security Survivor Challenge! We had four teams of brave DOE HQ employees willing to step up to the challenge of testing their cyber security survival skills during our October awareness event. Each team was quizzed on various multiple choice and true/false cyber security questions during a 10 minute round. To encourage audience participation, each team was given a 'life line' where they could refer to a coworker in the audience for assistance. After three entertaining rounds, we had the ultimate team of 'Internet' jungle survivors. The OCIO would like to thank all team contestants for participating in this fun, learning experience.

2009 Cyber Security Survivor Challenge Winners

HS-22 Green Computing Team

Steven Woodbury

Reisa Kall

Jeff Eagan

Beverly Whitehead

SAVE THE DATE

2010 Cyber Security Training Conference

May 17-20, 2010

Planning is underway for the 31st Department of Energy Cyber Security Training Conference to be held in Atlanta, Georgia, May 17 - 20, 2010. This year's theme, ***Cyber Security Innovation: Our Shared Responsibility***, focuses on ensuring that we continue to enable the DOE mission through ensuring adequate cyber security is in place, knowing cyber threats and vulnerabilities, and developing innovative approaches and programmatic strategies to protect Departmental information assets. The conference provides an excellent training opportunity for Federal and contractor employees to learn from DOE and industry experts and exchange cyber security information with other security and information technology professionals.

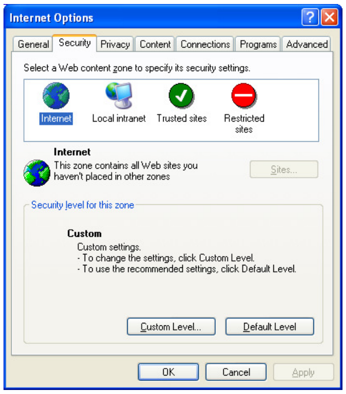
The conference committee is currently accepting abstract submissions and speaker biographies for conference presentations. Track presentations are planned for 45-minutes and training workshops can range from two hours to all-day sessions.

If you are interested in submitting an abstract, please visit: http://cio.energy.gov/csc_conference.htm for more information on the submission process.

Cyber Hero Answers Your Security Questions

Q: "Cyber Hero, I currently use Internet Explorer. At what level should I set my security and privacy settings?"

A: First, for those who wish to navigate along, open your Internet Explorer browser and go to the "Tools" menu, then select "Internet Options." You will see two tabs: one for "Security" and one for "Privacy". If you click on either tab, you will see buttons that say "Default Level" and "Default" (for the "Privacy" tab). While the default level of security is by no means the best choice, it should be the baseline choice: never minimum. Cyber Hero always prefers the higher-level settings; however, sometimes higher levels of security may impact your ability to view certain websites. Choose the highest level above "Default" that works for you.



Select a Web content zone to specify its security settings.

Internet
This zone contains all Web sites you haven't placed in other zones

Security level for this zone

Custom
Custom settings.
- To change the settings, click Custom Level.
- To use the recommended settings, click Default Level.